CLAIMS

[Claim(s)]
[Claim 1]
With the digital-watermarking circuit tester constituted so that one or the parameter beyond it relevant to digital watermarking relevant to contents might be detected
It is operationally combined with said digital-watermarking circuit tester, and has the authentication circuit tester constituted so that it might opt for the authentication corresponding to said contents based on one detected by said digital-watermarking circuit tester or the parameter beyond it, and one or the test criteria beyond it,
Said one or test criteria beyond it is a security system for protecting contents which is a thing based on the hope of the error relevant to said digital-watermarking circuit tester at the time of determining said one or parameter beyond it relevant to said digital watermarking.
[Claim 2]
Said one or test criteria beyond it includes the set of criteria to two or more test level of each,
Said authentication circuit tester is a security system according to claim 1 constituted so that the set of the following criteria may be chosen among said two or more test level when opting for the authentication based on the criteria set before the authentication circuit tester concerned is among said two or more test level goes wrong.
[Claim 3]
Each set of said test criteria is a test limitation corresponding to the count of min of the test which should be performed by said digital-watermarking circuit tester in order to opt for said authentication,
A security system including the failure limitation corresponding to the count of max of the failure for opting for authentication according to claim 2.
[Claim 4]
Said authentication circuit tester is a security system according to claim 3 which applies the next set of said criteria based on the result of said digital-watermarking circuit tester while having applied said former criteria set.
[Claim 5]
Said authentication circuit tester is a security system according to claim 3 which is not dependent on the result of said digital-watermarking circuit tester while having applied said former criteria set, and applies the next set of said criteria.
[Claim 6]
Said one or test criteria beyond it is a test limitation corresponding to the count of min of the test which should be performed by said digital-watermarking circuit tester in order to opt for said authentication,
A security system including the failure limitation corresponding to the count of max of the failure for opting for said authentication according to claim 1.
[Claim 7]
Said one or test criteria beyond it is a security system including the test limitation corresponding to the count of max of the test which should be performed by said digital-watermarking circuit tester in order to refuse said contents according to claim 1.
[Claim 8]
Said authentication circuit tester is a security system according to claim 1 constituted so that it may determine whether the whole data set exists based on digital watermarking relevant to the segment of a data set.
[Claim 9]

Said authentication circuit tester is a security system according to claim 8 constituted so that the random-segment of said data set may be chosen for a test with said digital-watermarking circuit tester.
[Claim 10]
Detection of the parameter beyond one or it relevant to digital watermarking relevant to contents,
Based on one or the parameter beyond it and one, or the test criteria beyond it, it has the decision of the authentication corresponding to said contents,
Said one or test criteria beyond it is the approach for protecting contents of being a thing based on the hope of the error relevant to detection of the parameter beyond one or it relevant to said digital watermarking.
[Claim 11]
Said one or test criteria beyond it includes the set of criteria to two or more test level of each,
The decision of said authentication is the approach according to claim 10 of including choosing the following criteria set among two or more test level, when opting for the authentication based on the criteria set of before of two or more test level goes wrong.
[Claim 12]
Each set of said test criteria is a test limitation corresponding to the count of min of the test which should be performed in order to opt for said authentication,
An approach including the failure limitation corresponding to the count of max of the failure for opting for said authentication according to claim 11.
[Claim 13]
The decision of said authentication based on the next set of said criteria is an approach including a result while having applied said former criteria set according to claim 11.
[Claim 14]
The decision of said authentication based on the next set of said criteria is an approach according to claim 11 independent of a result when having applied said former criteria set.
[Claim 15]
Said one or test criteria beyond it is a test limitation corresponding to the count of min of the test which should be performed in order to opt for authentication,
An approach including the failure limitation corresponding to the count of max of the failure for opting for said authentication according to claim 10.
[Claim 16]
Said one or test criteria beyond it is an approach including the test limitation corresponding to the count of max of the test which should be performed in order to refuse said contents according to claim 10.
[Claim 17]
The decision of said authentication is an approach according to claim 10 corresponding to the decision of whether said whole data set based on digital watermarking relevant to the segment of a data set exists.
[Claim 18]
An approach including selection of the random-segment of said data set according to claim 17.

[Translation done.]

(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2004-523799
(P2004-523799A)
(43)公表日　平成16年8月5日(2004.8.5)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G09C 5/00	G09C 5/00		5B017
G06F 12/14	G06F 12/14	320E	5J104

審査請求 未請求　予備審査請求 未請求　（全 25 頁）

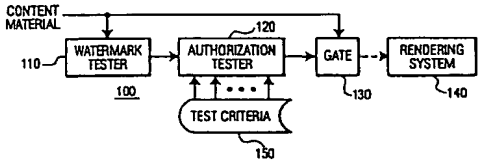
(21)出願番号　特願2002-568127(P2002-568127)
(86)(22)出願日　平成14年2月14日(2002.2.14)
(85)翻訳文提出日　平成14年12月12日(2002.12.12)
(86)国際出願番号　PCT/IB2002/000459
(87)国際公開番号　WO2002/069071
(87)国際公開日　平成14年9月6日(2002.9.6)
(31)優先権主張番号　60/271,400
(32)優先日　平成13年2月26日(2001.2.26)
(33)優先権主張国　米国(US)
(31)優先権主張番号　09/969,004
(32)優先日　平成13年10月2日(2001.10.2)
(33)優先権主張国　米国(US)
(81)指定国　EP(AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,TR),CN,JP,KR

(71)出願人　590000248
コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ
Koninklijke Philips Electronics N.V.
オランダ国　5621　ベーアー　アインドーフェン　フルーネヴァウツウェッハ　1
Groenewoudseweg 1, 5621 BA Eindhoven, The Netherlands
(74)代理人　100087789
弁理士　津軽　進
(74)代理人　100114753
弁理士　宮崎　昭彦

最終頁に続く

(54)【発明の名称】多重テストによるコピー保護

(57)【要約】
多階層のコピー保護方式は、電子透かし検出方式の誤りによるセキュリティ認証の失敗と、真のセキュリティ認証の失敗を識別する。最初のセキュリティレベルにおいてはフォールトトレランス性は低い。最初のセキュリティレベルにおいてセキュリティテストが失敗した場合、フォールトトレランス性が増加するが付加的な処理時間を要する、次のセキュリティレベルに処理が移行する。当該次のセキュリティレベルにおいても再びセキュリティテストが失敗した場合、フォールトトレランス性がより高いが、より付加的な処理時間を要する、より高いセキュリティレベルに処理が移行する。最終的に、セキュリティテストを合格しかつマテリアルがレンダリングされているか、又は実際にマテリアルがコピー保護されたものでかつ変更が許可されていないものであることを示して、失敗が電子透かし検出処理における失敗によるものでないと判断されるかの、いずれかとなる。



【特許請求の範囲】
【請求項１】
コンテンツに関連した電子透かしに関連するひとつ又はそれ以上のパラメータを検出するように構成された電子透かしテスターと、
前記電子透かしテスターと実施上結合され、前記電子透かしテスターによって検出されたひとつ又はそれ以上のパラメータと、ひとつ又はそれ以上のテスト基準とに基づき、前記コンテンツに対応する認証を決定するように構成された認証テスターとを有し、
前記ひとつ又はそれ以上のテスト基準は、前記電子透かしに関連した前記ひとつ又はそれ以上のパラメータを決定する際における前記電子透かしテスターに関連したエラーの見込みに基づくものである、コンテンツを保護するためのセキュリティシステム。
【請求項２】
前記ひとつ又はそれ以上のテスト基準は、複数のテストレベルそれぞれに対して基準のセットを含み、
前記認証テスターは、当該認証テスターが前記複数のテストレベルのうちの以前の基準セットに基づいた認証を決定することに失敗した場合に、前記複数のテストレベルのうち次の基準のセットを選択するように構成される、請求項１に記載のセキュリティシステム。
【請求項３】
前記テスト基準のそれぞれのセットは、前記認証を決定するために前記電子透かしテスターにより実行されるべきテストの最小回数に対応するテスト限界と、
認証を決定するための失敗の最大回数に対応する失敗限界とを含む、請求項２に記載のセキュリティシステム。
【請求項４】
前記認証テスターは、以前の前記基準セットを適用している間の前記電子透かしテスターの結果に基づいて、前記基準の次のセットを適用する、請求項３に記載のセキュリティシステム。
【請求項５】
前記認証テスターは、以前の前記基準セットを適用している間の前記電子透かしテスターの結果に依存せず、前記基準の次のセットを適用する、請求項３に記載のセキュリティシステム。
【請求項６】
前記ひとつ又はそれ以上のテスト基準は、前記認証を決定するために前記電子透かしテスターにより実行されるべきテストの最小回数に対応するテスト限界と、
前記認証を決定するための失敗の最大回数に対応する失敗限界とを含む、請求項１に記載のセキュリティシステム。
【請求項７】
前記ひとつ又はそれ以上のテスト基準は、前記コンテンツを拒絶するために前記電子透かしテスターにより実行されるべきテストの最大回数に対応するテスト限界を含む、請求項１に記載のセキュリティシステム。
【請求項８】
前記認証テスターは、データセットのセグメントに関連する電子透かしに基づいて、データセットの全体が存在するかどうかを決定するように構成される、請求項１に記載のセキュリティシステム。
【請求項９】
前記認証テスターは、前記電子透かしテスターによるテストのために、前記データセットのランダム的なセグメントを選択するように構成される、請求項８に記載のセキュリティシステム。
【請求項１０】
コンテンツに関連した電子透かしに関連するひとつ又はそれ以上のパラメータの検出と、
ひとつ又はそれ以上のパラメータ、及びひとつ又はそれ以上のテスト基準に基づき、前記コンテンツに対応する認証の決定とを有し、

前記ひとつ又はそれ以上のテスト基準は、前記電子透かしに関連したひとつ又はそれ以上のパラメータの検出に関連するエラーの見込みに基づくものである、コンテンツを保護するための方法。
【請求項１１】
前記ひとつ又はそれ以上のテスト基準は、複数のテストレベルそれぞれに対して基準のセットを含み、
前記認証の決定は、複数のテストレベルのうちの以前の基準セットに基いた認証を決定することに失敗した場合に、複数のテストレベルのうち次の基準セットを選択することを含む、請求項１０に記載の方法。
【請求項１２】
前記テスト基準のそれぞれのセットは、前記認証を決定するために実行されるべきテストの最小回数に対応するテスト限界と、
前記認証を決定するための失敗の最大回数に対応する失敗限界とを含む、請求項１１に記載の方法。
【請求項１３】
前記基準の次のセットに基づく前記認証の決定は、以前の前記基準セットを適用している間の結果を含む、請求項１１に記載の方法。
【請求項１４】
前記基準の次のセットに基づく前記認証の決定は、以前の前記基準セットを適用していたときの結果に依存しない、請求項１１に記載の方法。
【請求項１５】
前記ひとつ又はそれ以上のテスト基準は、認証を決定するために実行されるべきテストの最小回数に対応するテスト限界と、
前記認証を決定するための失敗の最大回数に対応する失敗限界とを含む、請求項１０に記載の方法。
【請求項１６】
前記ひとつ又はそれ以上のテスト基準は、前記コンテンツを拒絶するために実行されるべきテストの最大回数に対応するテスト限界を含む、請求項１０に記載の方法。
【請求項１７】
前記認証の決定は、データセットのセグメントに関連する電子透かしに基づく、前記データセットの全体が存在するかどうかの決定に対応する、請求項１０に記載の方法。
【請求項１８】
前記データセットのランダム的なセグメントの選択を含む、請求項１７に記載の方法。
【発明の詳細な説明】
【０００１】
本願は米国仮出願番号６０／２７１，４００（Ａｔｔｏｒｎｅｙ　Ｄｏｃｋｅｔ、ＵＳ００００４０、２００１年２月２６日出願）を含む。
【０００２】
【発明の属する技術分野】
本発明は、データ保護の分野、特に離れた場所からの不正なコピー行為からデータを保護することに関する。
【０００３】
【従来の技術】
データ保護はセキュリティの分野においてますます重要になってきている。多くの状況において、情報をコピーすること、さもなければ他の処理をする権限は、コピー保護されたマテリアル（ｍａｔｅｒｉａｌ）の、特定の特性についての符号化を評価することにより認証される。例えば、コピー保護されたマテリアルは、電子透かしを含むか又はコピー保護されたマテリアルであることを識別する他の符号化を含み、またマテリアルのこの特定のコピーが認証されたコピーであるかどうか、及び再コピー可能であるかどうかを識別するほかの符号化も含んでいる。また例えば、認証されたコンテンツ（ｃｏｎｔｅｎｔ　ｍ

ａｔｅｒｉａｌ）のコピーは、堅固な（ｒｏｂｕｓｔ）電子透かしと脆い（ｆｒａｇｉｌｅ）電子透かしとを含んでいる。堅固な電子透かしは、コンテンツの符号化と切り離せないように意図されている。電子透かしを除去しようとする試みはコンテンツに損傷を与える。脆い電子透かしはコンテンツが不正にコピーされた場合に損傷を受けるように意図されている。例えば、一般的な脆い電子透かしは、コンテンツが圧縮されたとき、又はその他の変更を受ける場合に損傷を受ける。このやり方によれば、インターネットを介して効果的に伝送されるように圧縮されたコンテンツは、堅固な電子透かしと、損傷を受けた脆い電子透かしとを伴って受信される。この例におけるコピー保護の権利を行使するために構成されたコンテンツ処理装置は、堅固な電子透かしの存在を検出し、脆い電子透かしが同時に存在していない場合には堅固な電子透かしを含むコンテンツの処理を妨げるように構成される。

【０００４】

【発明が解決しようとする課題】

電子透かしを符号化する処理と、対応する電子透かし検出の設計とは、相反する要求間のトレードオフを内包している。理想的な電子透かしは、コンテンツの通常のレンダリング（ｒｅｎｄｅｒｉｎｇ）の間は検出されず、一方では電子透かし検出器には容易に検出されるものであるべきである。電子透かし検出器による電子透かしの検出能力が向上すれば、通常のレンダリング時の検出能力も向上する。同様に、通常のレンダリング時の電子透かしの検出不可能性が減少すれば、電子透かし検出器による検出不可能性も減少する。従来の電子透かしを埋め込む処理は、その処理がコンテンツのレンダリングの質に影響を及ぼさないことを確実にするために、バイアスがかけられており、しばしば電子透かし検出器による検出能力を低下させている。即ち、電子透かし検出器が電子透かしを誤ってデコードしてしまう可能性は、僅かではない。従来の電子透かし検出処理は完全に信頼できるものではなく、フォールトトレラントな電子透かしに基づいたセキュリティの処理の存在が必要である。

【０００５】

本発明の目的は、信頼性が低い可能性のある電子透かし検出処理を考慮し、強固で信頼できるコピー保護方式を提供することにある。本発明の他の目的は、フォールトトレラントなコピー保護方式を提供することにある。

【０００６】

【課題を解決するための手段】

これらの目的及びその他の目的は、多層コピー保護方式によって実現される。最初のセキュリティレベルにおいては、フォールトトレランス性は低い。最初のセキュリティレベルにおいてセキュリティテストが失敗した場合、フォールトトレランス性は増加するが付加的な処理時間を要する、次のセキュリティレベルに処理が移行する。当該進んだセキュリティレベルにおいても再びセキュリティテストが失敗した場合、フォールトトレランス性はより高いが、より付加的な処理時間を要する、より高いセキュリティレベルに処理が移行する。最終的に、セキュリティテストを合格しかつマテリアルがレンダリングされているか、又は実際にマテリアルがコピー保護されたものでかつ変更が許可されていないものであることを示して、失敗が電子透かし検出処理における失敗によるものでないと判断されるかの、いずれかとなる。

【０００７】

本発明は、添付する図面を参照しながら例示の形で、以下により詳細に説明される。

【０００８】

【発明の実施の形態】

電子透かしのひとつ又はそれ以上のパラメータの符号化に基づくセキュリティ方式が幾つも知られており、将来さらなる電子透かしに基づくセキュリティ方式が開発されることが予想される。しかし一般的にこれらの方式は、電子透かし検出処理が信頼のできるものであることを前提としており、電子透かし検出処理が結果をレポートしたときに、当該レポートされた結果に基づきセキュリティ処理が制御を遂行する。

【０００９】
一般に電子透かし検出処理は１００％信頼できるものではないため、検出処理における誤りがセキュリティ処理によって誤った電子透かしと解釈され、コンテンツのレンダリングが不適切に終了する可能性がある。即ち、コンテンツはレンダリングが許可されたものであって、適切な電子透かしを含んでいたとしても、検出処理における失敗が、それが不適切な電子透かしであることや又は電子透かしが無いことを示唆してしまう可能性がある。同様に、より起こりにくいことではあるが、コンテンツが許可されたものではない可能性があっても、検出処理での失敗が、許可されたコンテンツであることを不適切にも示唆してしまったり、又はコンテンツがコピー保護されたものと認識することを失敗してしまう可能性がある。

【００１０】
本発明に従えば、電子透かし検出処理における誤りであるか、実際の電子透かし自体の誤りであるかを識別するための多レベルのセキュリティ処理が好適に利用できる。

【００１１】
図１は本発明によるセキュリティシステム１００のブロック図の例を示す。該システム１００は電子透かしテスター１１０、および当該電子透かしテスター１１０により提供される情報に基づき、入力されたコンテンツがレンダリングを認証されたものであるかどうかを決定する認証システム１２０を含む。本開示目的に関しては、「レンダリング」という語は、記録、送信、再生、変換などの、以降のコンテンツの伝送や処理のことも含む。前記認証テスターは、ゲート１３０とレンダリングシステム１４０との間に破線で示したように、コンテンツがレンダリングシステム１４０に提示されるかどうかを決定するゲート１３０を制御する。

【００１２】
本発明によれば、認証テスター１２０は、電子透かしテスター１１０により提供された情報が、レンダリングシステム１４０へのコンテンツの接続を正当化するものであるのか、又は切断を正当化するものであるのかを決定するためのテスト基準１５０を受信する。従来のセキュリティシステムにおいては、電子透かしテスター１１０からの情報は信頼できるものであり、正確なものであることを前提としていた。一方本発明では、レンダリング処理を妨害しないようにするための電子透かしの意図的な特性により、電子透かしテスターは本質的に信頼のできるものではなく、及び／又は、不正確なものであるいうことを前提としている。テスト基準１５０は特に、幾分信頼できない電子透かしテスター１１０と、コンテンツの不法なコピーとを識別するために設定される。

【００１３】
表１はテスト基準１５０の例の集合を示す。まずテストレベル１では、最大（テスト限界）３回の電子透かしテストが実行される。理想的には、これらの３つのテストは、もしテストされたコンテンツが適切な電子透かしを持つ場合にはそれぞれ「成功」という報告を返し、もしテストされたコンテンツが欠点のある、又は不適切な電子透かしを持つ場合には「失敗」という報告を返す。電子透かしテスト処理それ自体が欠点のあるものであることを鑑みて、表１のテスト基準「失敗限界」は、１回の失敗は許容されること示す。即ち、もしレベル１における３回の電子透かしテストのうち２回成功し、１回失敗した場合、認証テスター１２０はコンテンツは認証されたものであると宣言することになる。

【００１４】
【表１】

テストレベル	テスト限界	失敗限界
1	3	1
2	6	2
3	9	3

【００１５】
一方、もしテストレベル１が１回を超える失敗を示した場合には、認証テスター１５０は次のテストレベルに移行し、表１に示すテストレベル２に該当するテスト限界と失敗限界とを適用する。レベル２においては、最大６回の電子透かしテストが実行される。もし６回の電子透かしテストで２回かそれ未満の失敗が起こった場合には、認証テスター１５０はコンテンツが認証されたものであると決定する。もし２回を超える失敗が起こった場合には、認証テスター１５０は、９回のテストのうち失敗が３回を超えないことを要求する次のテストレベルに移行する。なお、追加のテストレベルはテスト基準１５０に含まれていても良いし、少なくても良い。このテスト手順は、はじめにどちらが起ころうとも、データが認証されたものであると判断されるまでか、又は最後のテストが完了するまで実行される。もし該データが認証されたものであると判断されることなく最後のテストが完了した場合、当該データは認証されていないものとして拒絶される。
【００１６】
前記テスト基準の特別な解釈は、前に行ったテストが以降のテストレベルにおける決定に影響を及ぼすようにするか否かによって変更しても良い。即ち例えば、表１のテスト限界及び失敗限界は累積の回数であっても良いし、表１のテスト限界と失敗限界はそれぞれのテストレベルに対して独立であっても良い。
【００１７】
累積の回数とする場合の例では、レベル１で２回目の失敗が起こった場合、本システムはレベル１のテストの履歴を保持したままレベル２に移行する。このように２回の失敗がすでに起こっているため、合計６回のテストが実行されるまで、コンテンツは続くそれぞれの電子透かしテストを合格しなければならない（レベル１において２回の失敗を起こしたテストの回数が２回又は３回であった場合、それぞれレベル２において４回又は３回のテストを失敗なしで通過する必要がある）。レベル２のテスト中に３回目の失敗が起こった場合、本システムはレベル３に移行し、コンテンツは残りのテストを合計９回のテストが完了するまで合格しなくてはならない。
【００１８】
独立の回数とする場合の例では、レベル１で２回目の失敗が起こった場合、システムはレベル２に移行し、更に６回のテストであと２回までの失敗を許容するテスト処理をリスタートする。
【００１９】
前記テスト基準の選択は、それぞれのレベルを通じた累積の回数によるテスト処理を選択する場合においても、それぞれのレベルにおいて独立の回数によるテスト処理を選択する場合においても、電子透かしテスター１１０が誤った結果を返す見込みの評価に依存して行う。電子透かしテスター１１０がほとんど誤った結果を返さない場合は、失敗限界はより低い値に設定することができる。反対に、電子透かしテスター１１０が頻繁に誤った結果を返す場合は、より高い失敗限界が妥当である。累積の回数によるテストは、前のテスト結果が破棄されないため、一般にテスト回数が少なくてすむ。
【００２０】
全てのテストレベルが適用されコンテンツがそれぞれのテストで失敗し続ける場合、認証テスター１５０はコンテンツが認証されたものでないと決定し、レンダリングシステム１

４０へのコンテンツ送信を妨げるためゲート１３０を制御する。

【００２１】

本発明の利用は、以下に示す出願中の米国特許出願「Ｐｒｏｔｅｃｔｉｎｇ Ｃｏｎｔｅｎｔ ｆｒｏｍ Ｉｌｌｉｃｉｔ Ｒｅｐｒｏｄｕｃｔｉｏｎ ｂｙ Ｐｒｏｏｆ ｏｆ Ｅｘｉｓｔｅｎｃｅ ｏｆ ａ Ｃｏｍｐｌｅｔｅ Ｄａｔａ Ｓｅｔ ｖｉａ Ｓｅｌｆ－Ｒｅｆｅｒｅｎｃｉｎｇ Ｓｅｃｔｉｏｎｓ」（Ａｎｔｏｎｉｕｓ Ａ．Ｍ．Ｓｔａｒｉｎｇ，Ｍｉｃｈａｅｌ Ａ．Ｅｐｓｔｅｉｎ，Ｍａｒｔｉｎ Ｒｏｓｎｅｒ，Ａｔｔｏｒｎｅｙ Ｄｏｃｋｅｔ、ＵＳ０００４０、シリアル番号０９／５３６９４４、２００２年３月２８日出願、参照により本明細に組み込まれたものとする）において示されている。この出願中の特許出願においては、データセット中のそれぞれのセクションが一意に識別され、該セクションの識別子がそれぞれのセクションに埋め込まれた電子透かしとして符号化される。より好ましくは堅固な電子透かしと脆い電子透かしとが組み合わされ埋め込まれる。データセットのある要素がレンダリングのために提示された場合、セキュリティシステムは、データセットのランダム的なセクションを要求し、当該ランダム的に選択されたセクションに適切な電子透かしがあることを認証する。ランダム的に選択された十分な数のセクションが認証された場合、データセット全体が存在すると決定される。もしデータセット全体が存在しない場合、ランダム的に電子透かしの無いセクションを選択する見込みは、データセット全体から失われたデータ量に比例する。このセキュリティ方式は大きなデータセットの選択されたセグメントの不正な配布を防止するためのものである。

【００２２】

デジタルオーディオ録音という面においては、例えば、コンプライアントな再生又は記録装置は、ランダム的な電子透かしテストを用いて、ＣＤのコンテンツ全体が存在しているという認証がないので、個々の曲をレンダリングすることを拒絶するように構成されている。圧縮されていないデジタルフォームによるＣＤのアルバム全部をダウンロードするのに要する時間は、ＤＳＬやケーブルモデムの速度であっても、ネットワークの負荷状況やそのほかの要因に依るが、１時間を超えるであろうと考えられる。このように、ＣＤのコンテンツ全体が存在していることを要求することにより、１時間を超えるダウンロードの「コスト」が掛かる状況において、インターネットにおける幅広いスケールの配布によって曲が盗まれる見込みはかなり減少する。

【００２３】

本発明によれば、図１のテスト基準１５０は要求されるセキュリティの程度、及び電子透かしテスト処理１１０の信頼性に基づいて決定される。一般に表１のテスト限界はデータセットの十分な数のサンプルが認証され、当該データセット全体が存在していることを保証できるように設定される。失敗限界は、電子透かしテスト処理１１０における偶発的なエラーによって、認証されるコンテンツが拒絶されないことを保証できるように設定される。テストを多レベルに分割することは、低い失敗率に基づきデータセットが存在していることが非常に明白となるときには、効果的なテストを行うためのものである。即ち、低いレベルのテストは好ましくは低い失敗率で構成され、そのため、もし電子透かしテストが信頼のできるものであるならば、コンテンツが認証されたものである場合には、低いレベルでのテストは該コンテンツをレンダリングする認証で終了する。次のレベルのテストを実行するための時間は、データセットの全体が存在しない場合か、又はコンテンツの早まった拒絶を避けるべきである場合にのみ費やされる。

【００２４】

図２は、本発明による多レベルの認証処理フロー図の例を示す。ステップ２１０において、例えば表１のレベル１のテストに対応する合格／失敗の決定基準の初期値が設定される。ステップ２２０において、電子透かしテストが実行され、合格／失敗の決定結果が出力される。

【００２５】

ステップ２３０において、ここまでの失敗の数が失敗限界を下回っていれば、ここまでで実行されたテストの数が評価される。ステップ２４０において、ここまでのテスト回数が

テスト限界を下回っていれば、ステップ２２０における次の電子透かしテストの実行へとループバックする。一方、ここまで実行されたテスト回数がテスト限界と同値であれば、ステップ２５０において、「認証されたものである」と結論し処理は終了する。

【００２６】

ステップ２３０において、ここまでの失敗の数が失敗限界に到達していれば、ステップ２６０において、さらなるテストレベルがあるか否かの決定が下される。もしない場合は、最後のテストが実行されていれば、ステップ２７０において、「認証されていないもの」と結論し処理は終了する。ステップ２６０において、さらなるテストレベルがあると判断された場合は、ステップ２８０において、次のテスト基準の集合が以前のテスト基準の集合と置き換えられ、ステップ２２０における次の電子透かしテストの実行へとループバックする。上述したように、ステップ２８０において、次のレベルのテスト基準が読み込まれたとき、以前のテストの回数と失敗の回数との累積は、各テストレベルで独立の回数を利用する方式の場合に破棄しても良いし、累積の回数を利用する場合に破棄しなくても良い。

【００２７】

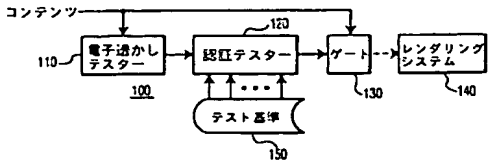
以上、単に本発明の原理を説明してきた。当業者は、本願に明白には記載又は示されていないようなものであっても、本発明の要旨及びその範囲内で本発明の原理を取り入れた様々な構成を工夫することが可能であることは理解されるであろう。例えば、図１のテスト基準１５０は、相対的に静的な基準の集合として示された。それぞれのレベルでのテスト基準が以前の実績によって決定されるか、又は電子透かしテスター１１０やその他の装置によって提供される「ノイズ値（ｎｏｉｓｅ ｆｉｇｕｒｅ）」や「品質値（ｑｕａｌｉｔｙ ｆｉｇｕｒｅ）」のような外部パラメータに基づいて決定される、適応型の（ａｄａｐｔｉｖｅ）テストを実行しても良い。ここで、該以前の実績としては、失敗限界が以前のエラー率に基づいて動的に設定される、電子透かしテスター１１０に関連したエラーの履歴（例えば、最終的に認証されたものであると決定されたマテリアルに対して報告された失敗の平均数）を含む。さらに、該以前の実績としては、テスト限界が以前の認証又は不認証の比率に基づいて動的に設定される、認証されていないマテリアルをレンダリングする試みの履歴を含む。これらシステム及びその他のシステムの構成と最適な特徴は、本開示内容を考慮すると当業者には明白であり、請求項に示す範囲に含まれる。

【図面の簡単な説明】

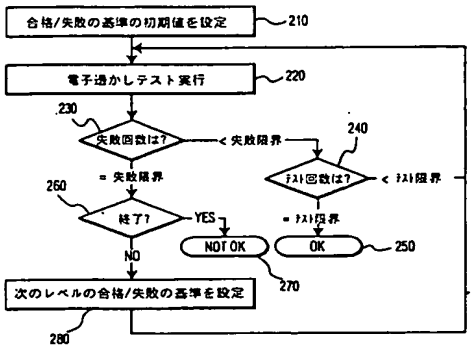
【図１】本発明によるセキュリティシステムのブロック図の例である

【図２】本発明によるセキュリティシステムのフロー図の例である

【図１】


コンテンツ
110
電子透かしテスター
100
120
認証テスター
テスト基準
150
ゲート
130
レンダリングシステム
140

【図２】


合格/失敗の基準の初期値を設定
210
電子透かしテスト実行
220
230
失敗回数は?
< 失敗限界
240
テスト回数は?
< テスト限界
= 失敗限界
260
終了?
YES
= テスト限界
NOT OK
OK
250
NO
270
次のレベルの合格/失敗の基準を設定
280